(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2004 (12.02.2004)

PCT

(10) International Publication Number
WO 2004/013986 A1

(51) International Patent Classification[7]: H04B 5/00, 7/00

(21) International Application Number:
PCT/US2003/022982

(22) International Filing Date: 24 July 2003 (24.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/212,193 2 August 2002 (02.08.2002) US

(71) Applicant: CISCO TECHNOLOGY, INC. [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventors: MEIER, Robert; 2975 Clear Creek Drive, Cuyahoga Falls, OH 44223 (US). OLSON, Timothy, J.; 5010 Tisdale Way, San Jose, CA 95130 (US). GRISWOLD, Victor; 2673 St. Albans Circle NW, North Canton, OH 44720 (US). YANG, Shemsung; 19580 Scotland Drive, Saratoga, CA 95070 (US). NELAKANTI, Bhavannarayana; 1422 Hawk Ct., Sunnyvale, CA 94087 (US).

(74) Agent: GARRED, John; Tucker, Ellis & West LLP, 1150 Huntington Building, 925 Euclid Avenue, Cleveland, OH 44115 (US).

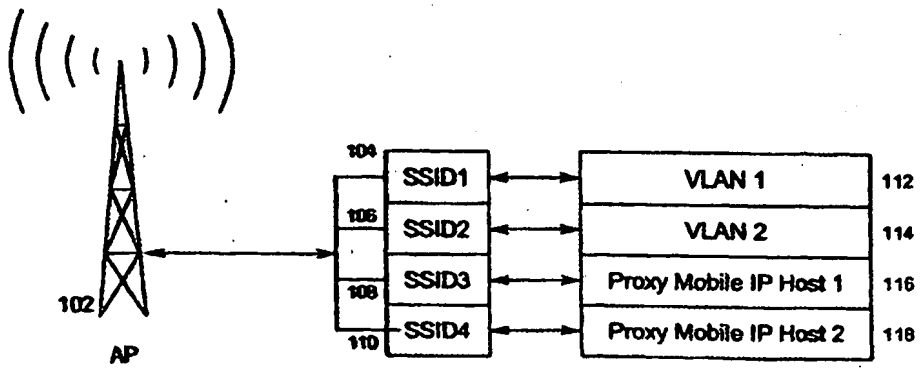
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: A METHOD FOR GROUPING 802.11 STATIONS INTO AUTHORIZED SERVICE SETS TO DIFFERENTIATE NETWORK ACCESS AND SERVICES



(57) Abstract: A method for associating a WSTA to a service set, wherein the service set is configurable at the AP. Each service set is an arbitrary grouping of one or more network service parameters, and is typically configured for either VLAN or proxy mobile IP host. When a wireless station desires to associate with an access point, the wireless station sends a message to the access point, the message containing a SSID. The access point then matches the SSID to a service set and associates the WSTA to either a home subnet or a VLAN based on the SSID. By locally configuring the service set, the default VLAN and home subnet for a WSTA may be different at each AP the WSTA encounters. A security server is configured with a list of allowed SSIDs for each wireless station to prevent unauthorized access to a VLAN or home subnet.

WO 2004/013986 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE OF THE INVENTION

A Method for Grouping 802.11 Stations into Authorized Service Sets to Differentiate Network Access and Services

BACKGROUND OF THE INVENTION

The present invention relates generally to network access and more particularly to a method and system to differentiate network access for different classes of users.

It is becoming increasingly important to differentiate network access for different classes of users, in particular different classes of wireless LAN users. One proposal for providing differentiated network access and services is that Access Points should implement a method wherein a Remote Authentication Dial-In User Server (RADIUS server) explicitly assigns an 802.11 station to a Virtual LAN identifier (VLAN ID) by returning a VLAN ID attribute in the RADIUS record for the station. Such RADIUS based VLAN assignment has limited scope and severely restricts mobility. A large or campus network may contain multiple VLANs that provide equivalent services. For example, a campus network may contain multiple Voice VLANS. If a RADIUS server explicitly assigns an 802.11 Voice over IP (VoIP) phone to a voice VLAN, then the phone is limited to a single voice VLAN, for example the phone may be limited to a VLAN on a single floor in a single building. The only method for segregating users is "VLAN trunking"; therefore, the proposal is generally limited to network areas with a VLAN infrastructure. Thus there exists a need for a method and system wherein multiple parameters can be grouped into a Service Set, which is controlled by a single RADIUS attribute that is not limited to a VLAN ID assignment.

For the purposes of describing the present invention, an "authorized WSTA" is any station that is explicitly authorized to access the network via a security server, and a "guest WSTA" is not explicitly authorized to access the network. A RADIUS server is used as an example security server in describing the present invention, but as those skilled in the art can readily appreciate the concepts of the present invention apply with any security server.

It should be noted that a "Service Set" as defined herein is not the same as an 802.11 Extended Service Set (ESS).

Additional objects, advantages and novel features of the invention will be set forth

in part in the description which follows, and in part will become apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention. The objects and advantages of the invention may be realized and attained by means of instrumentalities and combinations particularly pointed out in the appended claims.

BRIEF SUMMARY OF THE INVENTION

In view of the aforementioned needs, the invention contemplates a method for an access point to associate a wireless station to either a home subnet or a VLAN based on a configuration stored locally at the access point. When a wireless station desires to associate with an access point, the wireless station sends a message to the access point, the message containing a service set identifier (SSID), which is an arbitrary "name" for a service set. The access point then associates the wireless station to either a home subnet or a VLAN based on the SSID.

The method may also further comprise creating one or more service sets at the access point wherein each service set has a unique SSID. The access point upon receiving a message from a wireless station then matches the SSID of the message with a service set stored locally at the access point. After the access point confirms that it has a match for the SSID, the access point may then verify that the connection by the wireless station is authorized and that the station is authorized to use the SSID. This would typically be accomplished by using a security server such as a RADIUS server.

If the wireless station is currently bound to a remote home subnet, the access point enables communication between the wireless station and home subnet by tunneling to the home subnet. Alternatively, the access point may bind the wireless station to a home subnet that is local to the access point.

In an alternative embodiment, it is contemplated that the access point may send a list of subnets and/or VLAN's available for the SSID. The wireless station then selects a subnet or VLAN.

In another embodiment, the present invention contemplates a computer-readable medium instructions for an access point to associate a wireless station. The computer-readable medium comprising means for creating a service set at the access point. the computer-readable medium further comprising means for receiving a message from a

wireless station, the message containing an SSID. The computer-readable medium also comprising means for verifying the access point has a matching service set for the SSID. The computer-readable medium further comprises means for authenticating a wireless station by accessing a security server that is communicatively coupled to the access point. The computer-readable medium having means for associating the wireless station to either a VLAN or a home subnet based on the SSID. In an alternative embodiment, the security server returns a list of one or more SSIDs for which the station is authorized. The station is prevented from accessing the network if its SSID does not match one of the SSIDs in the list returned by the security server.

The present invention further contemplates an access point, comprising means for assigning one of the group selected from a VLAN and a subnet to a service set; means suitably adapted for receiving a message from a wireless station, the message further comprising a SSID; means suitably adapted to match the SSID to the service set; means suitably adapted for authenticating a wireless station by accessing a security server; means for associating the wireless station to one of the group consisting of a home subnet or VLAN based on the SSID, wherein the service set home subnet or VLAN parameter is configured locally at the access point.

The access point may also further comprise means for binding the wireless station to the home subnet, means for tunneling to the home subnet. In the alternative, the access point may have means for binding the wireless station to a local subnet.

In yet another embodiment, the present invention contemplates an access point, comprising means for creating a service set at the access point; means for accessing the access point by sending a message from the wireless station to the access point, the message comprising a SSID; means for verifying the access point has a matching service set for the SSID; means for authenticating the wireless station by the access point accessing a security server that is communicatively coupled to the access point; means for providing the wireless station with a list of subnets available for the SSID; and wherein the service set is configured locally at the access point.

The present invention also contemplates an 802.11 network, comprising a first basic service set comprising a first access point, and a second basic service sets, comprising a second access point. The first access point comprises means for creating a service set at

the first access point; means for receiving a message from the wireless station to the first access point, the message comprising a SSID; means verifying the first access point has a matching service set for the SSID; and means for associating the wireless station to a first home subnet based on the SSID. The second access point comprises means for creating a service set at the second access point; means for receiving a message from the wireless station to the second access point, the message comprising the SSID used in the message to the first access point; means verifying the second access point has a matching service set for the SSID; and means for associating the wireless station to a second home subnet based on the SSID, wherein the first home subnet is different than the second home subnet.

In another embodiment, the present invention contemplates an 802.11 network, comprising a first basic service set comprising a first access point, and a second basic service sets, comprising a second access point. The first access point comprises means for creating a service set at the first access point; means for receiving a message from the wireless station to the first access point, the message comprising a SSID; means verifying the first access point has a matching service set for the SSID; and means for associating the wireless station to a first VLAN based on the SSID. The second access point comprises means for creating a service set at the second access point; means for receiving a message from the wireless station to the second access point, the SSID used in the message to the first access point; means verifying the second access point has a matching service set for the SSID; and means for associating the wireless station to a second VLAN based on the SSID, wherein the first VLAN is different than the second VLAN.

Among those benefits and improvements that have been disclosed, other objects and advantages of this invention will become apparent from the following description taken in conjunction with the accompanying drawings. The drawings constitute a part of this specification and include exemplary embodiments of the present invention and illustrate various objects and features thereof.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The drawings illustrate the best mode presently contemplated of carrying out the invention.

This the drawings:

FIG 1 is a block diagram illustrating the relationship between an AP, SSID and VLAN or Proxy Mobile IP Host as contemplated by the present invention;

FIG 2 is a block diagram illustrating a wireless station moving from one basic service set controlled by a first access point set to a second basic service set controlled by a second access point;

FIG 3 is a block diagram illustrating the communications between a wireless station, access point, and a security server when a wireless station attempts to gain entry to a network;

FIG 4 is a block diagram illustrating the steps for configuring an access point for use with the present invention;

FIG 5 is a block diagram showing the steps for a wireless station to associate with an access point..

DETAILED DESCRIPTION OF INVENTION

The present invention contemplates a method where wireless stations (WSTAs) are partitioned into "Service Sets." A Service Set Identifier (SSID) identifies each service set. The SSID can be a standard 802.11 SSID.

A Service Set is an arbitrary grouping of one or more network service parameters. Service parameters may be used to differentiate network access for security purposes. For example, "guest" WSTAs that are restricted to secure "guest" subnets may be grouped into a "GUEST" Service Set. Service parameters may also be used to differentiate network services that are not necessarily related to security. For example, employee WSTAs that require a "Proxy Mobile IP" service for seamless campus mobility may be grouped into a "MOBILE-EMPLOYEE" Service Set.

Service Set authorization is accomplished in one of two ways. While the following examples use a RADIUS server, as those skilled in the art can readily appreciate, the authorization may be accomplished with any security server. First a RADIUS server can explicitly authorize a WSTA to join one or more Service Sets. In the first case, the RADIUS server returns a list of allowed SSID's in the RADIUS record for the WSTA. For backward compatibility with legacy 802.11 systems the absence of the SSID list can be

interpreted asa list of all SSIDs. Second, a RADIUS server can explicitly assign a WSTA to a Service Set. In that case, the RADIUS server returns an "assigned SSID" in the RADIUS record for the WSTA. Note that the first method enables the WSTA to change its active Service Set without requiring configuration changes to the RADIUS database.

A standard 802.11 WSTA sends an association message, which contains an 802.11 SSID, each time it associates with a parent AP. A WSTA is only associated if it successfully passes any authentication criteria that is defined for its SSID, and the WSTA is authorized to join the Service Set identified by its SSID or is explicitly assigned to a different SSID by the RADIUS server.

Unauthenticated "guest WSTAs" are assigned to a default guest Service Set, which may permit restricted access to the network.

Service set parameter values that determine a WSTA's home subnet are configured locally in wireless access points (APs) so that parameter values have local significance. For example, a campus network may have a voice VLAN in each building. A "VOICE" SSID can be bound to VLAN 10 in building 1 and VLAN 20 in building 2. A WSTA configured with the "VOICE" SSID can access any voice VLAN.

AP's determine current Service Set parameter values from SSID configuration values and WSTA 'context' information. For example, a WSTA may belong to a Service Set named "MOBILE" that has "seamless inter-subnet mobility" enabled. A "home subnet" may be configured for the "MOBILE" SSID in each AP. Initially, a "MOBILE" WSTA is bound to the home subnet configured for "MOBILE" in its parent AP. Thereafter, as the WSTA roams, it is seamlessly bound to its original home subnet, regardless of the "home subnet" configured for "MOBILE" in any new parent AP. A context transfer protocol is used to transfer the WSTA's home subnet context to a new parent AP.

The home subnet bindings for a "MOBILE" WSTA can be aged and discarded after the WSTA becomes inactive for some period of time so that the WSTA can be bound to a different, more optimal, home subnet when it becomes active again.

A WSTA's home subnet can be automatically derived by "snooping" the source IP address in IP packets transmitted by the WSTA rather than using an access point service set parameter value to bind the WSTA to a home subnet. In that case, an SSID/home-subnet

database is used to determine if the WSTA is authorized to access the home subnet that corresponds to its IP address. The SSID/home-subnet database contains a list of "allowed" subnets for each SSID. The database can be statically configured. Alternatively, APs can automatically determine the subnet address for each subnet that is accessible via one of its configured SSIDs. Note that the subnet address for an SSID may not be the same in different APs. The list of allowed subnets for each SSID is the aggregate of the local SSID/subnet bindings in all APs. (This method is necessary to support WSTA's with a permanet IP address. It is also necessary to re-establish home subnet bindings that have been aged and discarded.)

By using the Service Set method as described herein, a WSTA can be assigned to a specific VLAN ID. However this method is not limited to VLAN ID assignment. Instead, multiple parameters can be grouped into a single Service Set, which may be controlled by a single RADIUS or other security server attribute. Because the Serve Set parameters are instantiated locally in parent AP's, the Service Set parameters can be set to values that are optimal for the local network topology and current WSTA context. For example, either VLAN trunking or Proxy Mobile IP tunneling can be used, as is locally appropriate, to restrict guest WSTAs to a secure guest subnet.

Another feature that may be incorporated with the present invention is that a WSTA can change its Service Set without requiring changes to its RADIUS configuration. For example, a WSTA can inhibit seamless mobility, for example when it is running a non-IP application that prohibits inter-subnet mobility, by changing its active SSID to one that does not have Proxy Mobile IP enabled.

The method of the present invention may be implemented by using the standard 802.11 SSID, therefore, no changes are required to existing to WSTAs to obtain the benefits of the present invention.

Referring now to Figure 1, there is shown an AP 102. The AP 102 as shown has for SSID numbers, 104, 106, 108, 110. Each SSID number 104, 106, 108, 110 has a corresponding parameter 112, 114, 116, 118 assigned to it. For example, the AP 102 will associate VLAN1 112 with SSID1 104 VLAN2 114 with SSID2 106, Prox Mobile IP Home Agent 1 116 with SSID3 108, and Proxy Mobile IP Home Agent 2 118 with SSID4 110.

Figure 2 shows an Extended Service Set (ESS) 200. The ESS comprises two basic service sets (BSS) 204 and 206. AP 102 controls BSS 204 and AP 202 controls BSS 206. A WSTA 208 is shown that travels a path 212 from BSS 204 to BSS 206. As contemplated by the present invention, when WSTA 208 associates with each AP 102 and 202, it sends an SSID (not shown) to the AP 102 or 202. Because each AP is individually configured, when WSTA is associated with AP 202 it may be bound to a different VLAN or Proxy Mobile IP Home Agent than it was when it was associated with AP 102.

Referring now to Figure 3 there is shown a WSTA 302 attempting to gain access to AP 102. A message is sent from WSTA 302 to the AP 102. The AP 102 then attempts to authenticate the WSTA 302 by sending authentication message 306 comprising the WSTA 302 and the WSTA's SSID to security server 304. If the security server 304 authenticates WSTA 302, it then sends a message 308 containing parameters for the WSTA 302 to the AP 102.

Figure 4 shows an exemplar of a method that can be used for configuring an AP for use with the present invention. The process begins by defining a configuration at step 402. At step 404 the authentication criteria is defined. At step 406 the Service Sets and Identifiers are defined. Then as shown at step 408, for each ID which may be done either at the same time the for Service Set are defined or separately, the parameters for each SSID are defined. As shown in step 410 Proxy Mobile IP is either configured or disabled for each SSID. As shown in step 412, if Proxy Mobile IP is enabled, then the default home subnet is configured as shown at step 414. If Proxy Mobile IP is disabled, then the default VLAN ID is configured as shown at 416. If there are more Service Sets to configure, then as shown in step 418 processing returns to step 410, otherwise, as shown in step 420 the process is completed.

In Figure 5 there is shown a procedure 500 contemplated by the present invention for a WSTA 208 to associate with an AP 102. Beginning at step 502, the WSTA 208 accesses the AP 102 by sending a message to the AP 102, the message including a SSID (SSID). As shown in step 504, the AP 102 checks to ascertain if it has a matching SSID. If the AP 102 does not have a matching SSID, then as shown in step 506 the AP 102 does not allow the connection.

If the AP 102 does have a matching SSID, then the AP determines at step 508 if the

association is allowed for the WSTA 208. This can be done by accessing a security server, such as a RADIUS server. For example, when the RADIUS server is accessed, the RADIUS server returns a list of allowed SSIDs. The association for the WSTA is only allowed if the WSTA's SSID is in the list. This prevents unauthorized access to a service set that is supported in the AP. If the association is not allowed, then at step 510 the AP does not allow the connection.

If the AP 102 does have a matching SSID and the WSTA 208 is allowed to associate, then the AP 102 determines whether to associate the WSTA 208 by Subnet or VLAN. If the association is by subnet, then the AP 102 binds the WSTA 208 to the home subnet 514. At step 516 the AP 102 determines if it can tunnel to the home subnet, if it can than the process is completed as shown in step 518.

If the AP 102 can not tunnel to the home subnet at step 516, then the AP 102 can bind the WSTA 208 to a local subnet as shown in step 520. Then as shown in step 518, the process is completed.

If at step 512 it is determined that the WSTA 208 is to be bound to a VLAN, then the procedure goes to step 522 wherein the WSTA 208 is bound to a VLAN. Then the procedure is completed as shown in step 518.

While in the description of the process of Figure 5 the process terminates after associating the WSTA 208 to either a subnet or VLAN, as those skilled in the art can readily appreciate, other parameters may be configured at this point in time. As the WSTA 208 associates with another AP 202, the process is repeated. Because each AP 102, 202 has its own separate bindings for the Service Sets, when a WSTA 208 moves from one AP 102, to another AP 202, the VLAN or subnet that the WSTA 208 is bound to may change.

Although the invention has been shown and described with respect to a certain preferred embodiment, it is obvious that equivalent alterations and modifications will occur to others skilled in the art upon the reading and understanding of this specification. The present invention includes all such equivalent alterations and modifications and is limited only by the scope of the following claims.

CLAIM(S)

What is claimed is:

1. A method for an access point to associate a wireless station, the steps comprising:

receiving a message from a wireless station, the message comprising a service set identifier; and

associating the wireless station to a service set, where a service set defines a set of network access parameter values and

wherein a service set parameter value is configured locally at the access point.

2. The method of claim 1 further comprising grouping wireless stations into service sets, with each service set having a unique service set identifier.

3. The method of claim 1 further comprising configuring a list of service set identifiers at the access point, wherein a different set of service set parameter values is associated with each of the access point's service set identifiers.

4. The method of claim 1 further comprising verifying the access point has a matching service set for the service set identifier sent by the wireless station.

5. The method of claim 3 wherein the service set identifier is an 802.11 service set identifier.

6. The method of claim 1 further comprising authenticating the wireless station by the access point accessing a security server communicatively coupled to the access point.

7. The method of claim 6 wherein the security server is a Remote Authentication Dial-In User Server.

8. The method of claim 7 further comprising authenticating that the wireless

station is authorized to use the service set identifier configured on the wireless station.

9. The method of claim 8 further comprising authenticating that the wireless station is authorized to use its service set identifier via an allowed service set identifier list contained in the RADIUS record for the wireless station.

10. The method of claim 1 further comprising binding the wireless station to a home subnet, based on a service set parameter value that identifies the home subnet.

11. The method of claim 10 further comprising tunneling the station to the home subnet.

12. The method of claim 11 further comprising a tunneling method where a proxy mobile IP entity in the network infrastructure establishes a Mobile IP tunnel to the home subnet for a Mobile IP unaware wireless station.

13. The method of claim 1 further comprising a method where a service set parameter is used to determine whether a wireless station requires proxy Mobile IP tunneling services.

14. The method of claim 13 further comprising a method wherein the home subnet for a wireless station is automatically determined by examining the source IP address in IP packets transmitted by the wireless station.

15. The method of claim 13 further comprising a method for verifying that the wireless station is authorized to access the home subnet. wherein at least one access point is configured with an service set identifier and corresponding server set parameter value that identifies the home subnet.

16. The method of claim 1 further comprising binding the wireless station to an Ethernet VLAN, based on a service set parameter that is configured with a VLAN

Identifier.

17. The method of claim 16 further comprising bridging the station to the VLAN on a wired or wireless VLAN trunk link attached to the access point, where all frames transmitted on the VLAN trunk link contain an explicit or implicit VLAN Identifier.

18. A method for an 802.11 access point to associate an 802.11 wireless station, the steps comprising:

creating a service set at the access point;

receiving a message from the wireless station by the access point, the message comprising an 802.11 SSID;

verifying the access point has a matching service set for the 802.11 service set identifier;

authenticating the wireless station by the access point accessing a security server communicatively coupled to the access point; and

associating the wireless station to one of the group consisting of a home subnet and a VLAN based on the service set identifier;

wherein the service set parameter values is configured locally at the access point.

19 The method of claim 18 further comprising, binding the wireless station to the home subnet.

20. The method of claim 18 further comprising a method where the wireless station is bound to the same home subnet, even when it roams to an AP with a different VLAN ID or home subnet identifier configured for the service set identifier.

21. The method of claim 20 further comprising discarding the home subnet bindings for the wireless station after some period of inactivity so that the station can be bound to a diffemet subnet when it again becomes active.

22. The method of claim 20 further comprising a method selected from one of the

group consisting of wherein VLAN trunking is used to access the home subnet on access points that have a VLAN trunk link to the home subnet, and a Proxy Mobile IP tunnel is used to access the home subnet.

23. The method of claim 18 further comprising tunneling to the home subnet.

24. The method of claim 18 further comprising binding the wireless station to a local subnet.

25. A method for an 802.11 wireless station to associate with an 802.11 access point, the steps comprising:

creating a service set at the access point;

receiving a message from the wireless station by the access point, the message comprising a 802.11 service set identifier;

verifying the access point has a matching service set for the service set identifier;

authenticating the wireless station by the access point accessing a security server;

providing the access point with a list of service set identifiers that are permitted for the wireless station; and

wherein the service set is configured locally at the access point.

26. A computer-readable medium of instructions for an 802.11 access point to associate an 802.11 wireless station, the steps comprising:

means for creating a service set at the access point;

means for access point to receive a message from the wireless station, the message comprising an 802.11 service set identifier;

means for verifying the access point has a matching service set for the 802.11 service set identifier;

means for authenticating the wireless station by the access point accessing a security server communicatively coupled to the access point;

means for associating the wireless station to one of the group consisting of a home subnet and a VLAN based on the service set identifier;

wherein the service set is configured locally at the access point.

27. The computer-readable medium of instructions as in claim 26 further comprising, means for binding the wireless station to the home subnet.

28. The computer-readable medium of instructions as in claim 26 further comprising means for tunneling to the home subnet.

29. The computer-readable medium of instructions as in claim 26 further comprising means for binding the wireless station to a local subnet.

30. A computer-readable medium of instructions for an 802.11 wireless station to associate with an 802.11 access point, the steps comprising:

means for creating a service set at the access point;

means for the access point to receive a message from the wireless station, the message comprising a service set identifier;

means for verifying the access point has a matching service set for the service set identifier;

means for authenticating the wireless station by the access point accessing a security server;

means for providing the wireless station with a list of subnets available for the service set identifier;

wherein the service set is configured locally at the access point.

31. A computer-readable medium having stored thereon instructions which when executed by a processor, cause the processor to perform the steps comprising of:

creating a service set at the access point;

receiving a message from the wireless station, the message comprising an 802.11 service set identifier;

verifying the access point has a matching service set for the 802.11 service set identifier;

authenticating the wireless station by the access point accessing a security server that is communicatively coupled to the access point;

associating the wireless station to one of the group consisting of a home subnet and a VLAN based on the service set identifier; and

wherein the service set is configured locally at the access point.

32. The computer-readable medium as in claim 31 further comprising, instructions for binding the wireless station to the home subnet.

33. The computer-readable medium as in claim 31 further comprising instructions for tunneling to the home subnet.

34. The computer-readable medium of instructions as in claim 31 further comprising instructions for binding the wireless station to a local subnet.

35. A computer-readable medium having stored thereon instructions which when executed by a processor, cause the processor to perform the steps comprising of:

creating a service set at the access point;

receiving a message from the wireless station to the access point, the message comprising a service set identifier;

verifying the access point has a matching service set for the service set identifier;

authenticating the wireless station by the access point accessing a security server that is communicatively coupled to the service point; and

providing the access point with a list of service set identifiers that are permitted for the wireless station ; and

wherein the service set is configured locally at the access point.

36. An access point, comprising

means for assigning one of the group selected from a VLAN and a subnet to a service set;

means suitably adapted for receiving a message from a wireless station, the message

further comprising a service set identifier;

means suitably adapted to match the service set identifier to the service set;

means suitably adapted for authenticating a wireless station by accessing a security server;

means for associating the wireless station to one of the group consisting of a home subnet and a VLAN based on the service set identifier;

wherein the service set is configured locally at the access point.

37. The access point as in claim 36 further comprising, means for binding the wireless station to the home subnet.

38. The access point as in claim 37 further comprising means for tunneling to the home subnet.

39 The access point as in claim 36 further comprising means for binding the wireless station to a local subnet.

40. The access point as in claim 36 wherein the access point is an 802.11 access point.

41. An access point, comprising:

means for creating a service set at the access point;

means for accessing the access point by sending a message from the wireless station to the access point, the message comprising a service set identifier;

means verifying the access point has a matching service set for the service set identifier;

means for authenticating the wireless station by the access point accessing a security server that is communicatively coupled to the access point;

means for providing the access point with a list of service set identifiers that are permitted for the wireless station ; and

wherein the service set is configured locally at the access point.

42. The access point as in claim 41 wherein the access point is an 802.11 access point.

43. An 802.11 network, comprising:

a first basic service set comprising a first access point, and a second basic service sets, comprising a second access point;

wherein the first access point comprises

means for creating a service set at the first access point;

means for receiving a message from the wireless station to the first access point, the message comprising a service set identifier;

means verifying the first access point has a matching service set for the service set identifier;

means for associating the wireless station to a first home subnet based on the service set identifier; and

wherein the second access point comprises

means for creating a service set at the second access point;

means for receiving a message from the wireless station to the second access point, the message comprising the service set identifier used in the message to the first access point;

means verifying the second access point has a matching service set for the service set identifier;

means for associating the wireless station to a second home subnet based on the service set identifier;

wherein the first home subnet is different than the second home subnet.

44. An 802.11 network, comprising:

a first basic service set comprising a first access point, and a second basic service sets, comprising a second access point;

wherein the first access point comprises

means for creating a service set at the first access point;

means for receiving a message from the wireless station to the first access point, the message comprising a service set identifier;

means verifying the first access point has a matching service set for the service set identifier;

means for associating the wireless station to a first VLAN based on the service set identifier; and

wherein the second access point comprises

means for creating a service set at the second access point;

means for receiving a message from the wireless station to the second access point, the service set identifier used in the message to the first access point;

means verifying the second access point has a matching service set for the service set identifier;

means for associating the wireless station to a second VLAN based on the service set identifier;

wherein the first VLAN is different than the second VLAN.

45. A method wherein Wireless stations (WSTAs) are partitioned into Service Sets, each Service Set comprising a Service Set Identifier and a network access parameter value, comprising the steps of:

configuring an AP with a list of at least one service set identifier that identifies the service set the AP will accept;

sending a message from the WSTA to its parent AP, the message comprising an active service set identifier for the WSTA, wherein the service set identifier is selected from the group consisting explicitly identifying a service set, and a wildcard so that the WSTA's service set is selected by a network infrastructure;

verifying by the parent AP that the parent AP has an service set identifier that matches the service set identifier sent by the WSTA; and

authorizing the WSTA to use its service set identifier by a security server and a security protocol;

wherein service set parameters that determine the WSTA's at least one of the group consisting of VLAN and home subnet may be configured with different values for the same

service set identifier in a different AP.

46. The method of claim 45 wherein the security server is a RADIUS server and the security protocol is RADIUS.

47. The method in claim 46 further comprising a method wherein a list of allowed service set identifiers for a WSTA is sent from the RADIUS server to the parent AP in a RADIUS protocol message.

48. The method in claim 46 further comprising a method where a RADIUS server explicitly assigns a WSTA to a service service by including an service set identifier in a RADIUS protocol message sent to the parent AP.

49. The method in claim 45 wherein a service set parameter that determines the WSTA's home subnet contains at least one of a VLAN Identifier and an IP subnet address.

50. The method in claim 49 further comprising a method where a WSTA is initially bound to a home subnet based on the service set parameter value in its parent AP, but the service set parameter is not used to bind the WSTA to a different home subnet as the WSTA roams to APs with a different service set parameter value, so that the WSTA is bound to a single home subnet as it roams.

51. The method in claim 50 where either VLAN trunking or IP tunneling is dynamically selected to bind a station to a single home subnet as it roams, so that the most optimal available access method is used to forward packets between the WSTA and its home subnet.

52. The method in claim 50 further comprising discarding home subnet bindings for a WSTA after the WSTA has become inactive for some period of time, so that the WSTA can bind to a different (i.e. more optimal) subnet when it again becomes active.

53. The method in claim 49 further comprising a method where a WSTA is bound to a different home subnet when it roams to an AP with a different service set parameter value, so that the WSTA is bound to the "optimal" home subnet.

54. The method in claim 45 where a WSTA uses a "wildcard" service set identifier to match a different service set identifier in the parent AP.

55. The method in claim 45 where the service set parameter that determines the WSTA's home subnet contains a Mobile IP home agent address.

56. The method in claim 45 further comprising a method wherein a service set parameter is used to determine whether a WSTA should be bound to a single home subnet as it roams in a network with multiple subnets.

57. The method in claim 56 wherein a service set parameter is used to determine whether Proxy Mobile IP and Mobile IP tunneling is used to bind a station to a single home subnet.

58. The method in claim 56 wherein the home subnet for a WSTA is determined by examining the IP address in IP packets transmitted by the WSTA.

59. The method in claim 58 further comprising a method wherein a station is not bound to a home subnet unless it is authorized to access that home subnet.

60. The method in claim 59 wherein a WSTA is authorized to access a home subnet only when there is at least one AP that has a parameter value for the services set identified by the WSTAs service set identifier that contains at least one of a VLAN ID and subnet address that identifies the home subnet.

61. The method in claim 60 where a central database is used to authorize a WSTA to access a home subnet, wherein the central database contains a list of service set

identifiers and, for each service set identifier, a list of allowed subnets.

62. The method in claim 61 where the list of subnets for each service set identifier is statically configured or automatically populated with the local service set identifier and subnet bindings for each AP.

63. The method in claim 45 wherein an unauthenticated WSTA is assigned to a guest service set and where service set parameter values, configured for the guest service set at least 1 APs, are used to restrict the WSTA to at least one guest subnets.

64. The method in claim 45 wherein a WSTA is authorized to use more than one service set identifier so that the WSTA can change its service set without requiring configuration changes in the security server.

65. The method in claim 45 wherein the service set identifier is an 802.11 service set identifier and a wildcard service set identifier is an 802.11 broadcast service set identifier.

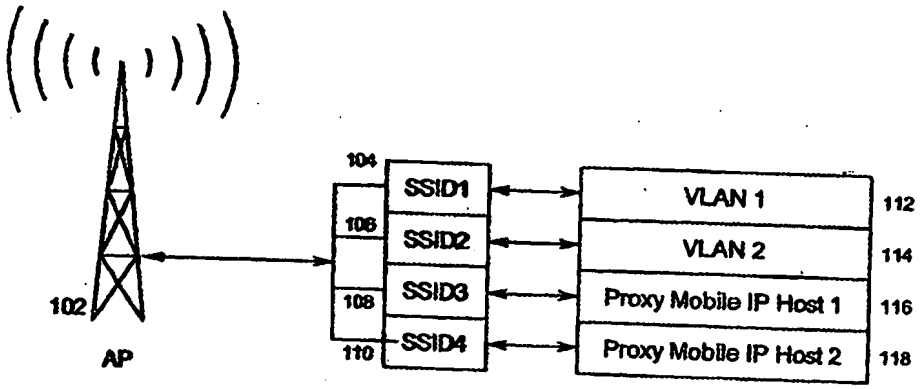

102
AP
104
SSID1
106
SSID2
108
SSID3
110
SSID4
VLAN 1
112
VLAN 2
114
Proxy Mobile IP Host 1
116
Proxy Mobile IP Host 2
118

Fig. 1

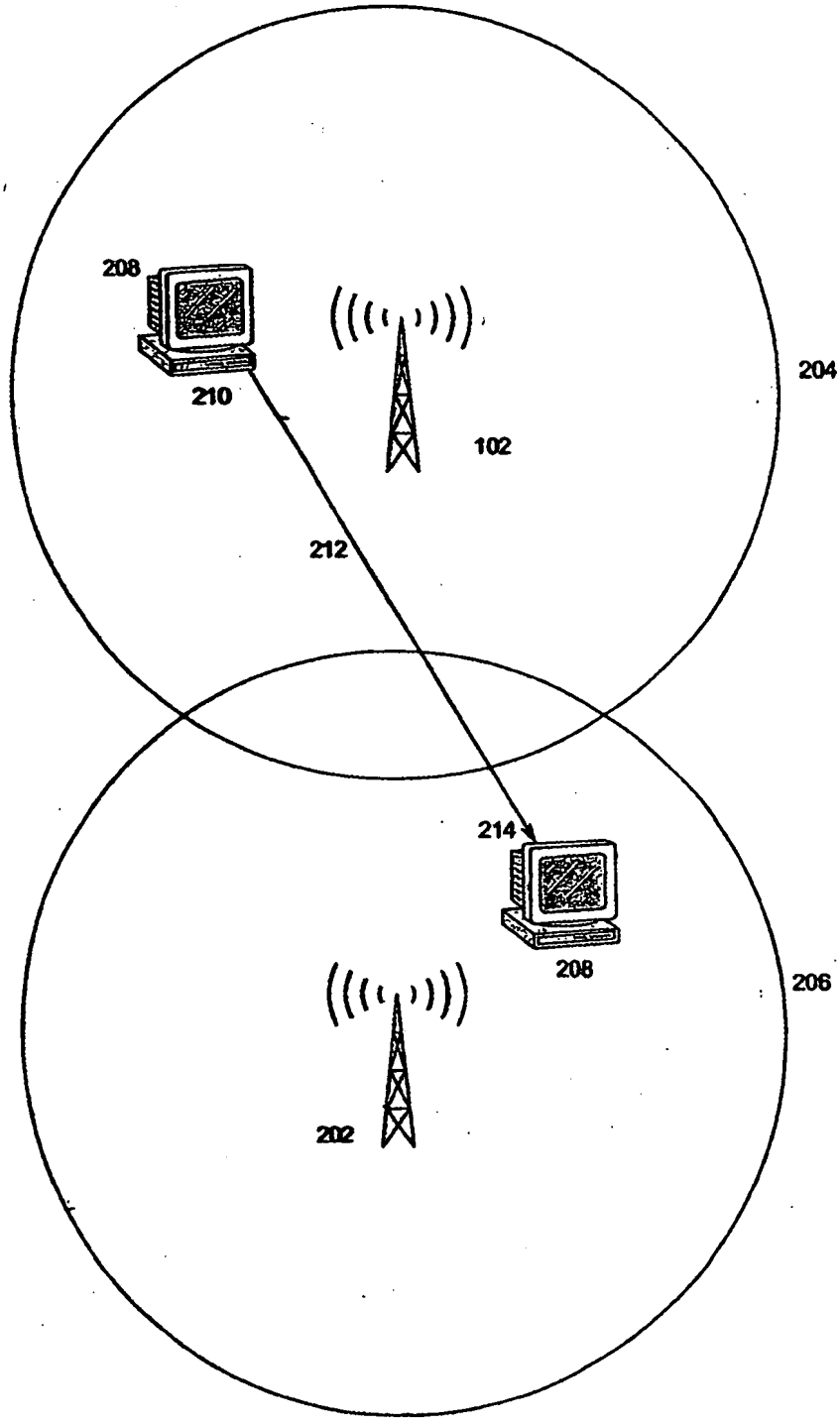


Fig. 2

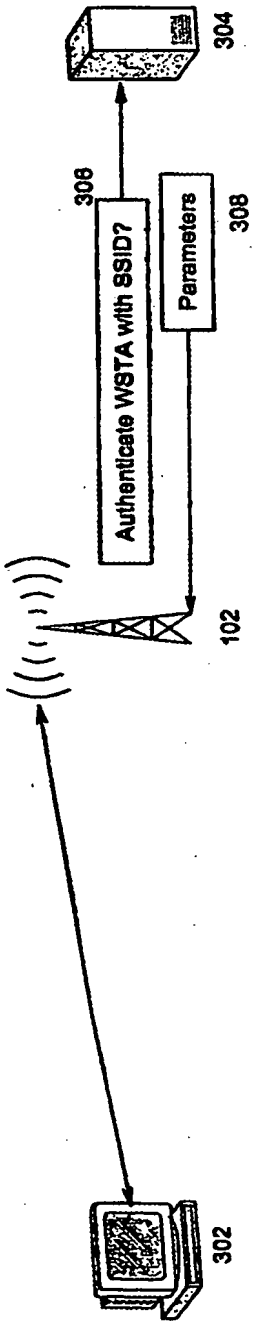


Fig. 3

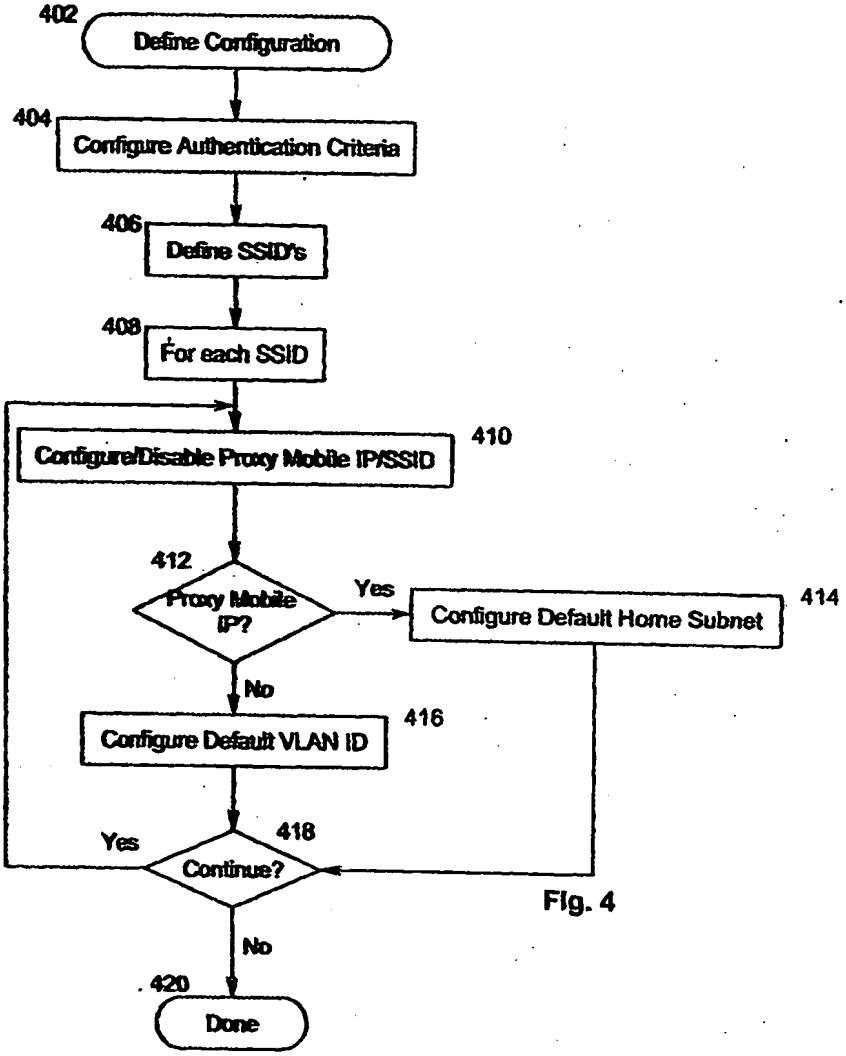

402
Define Configuration
404
Configure Authentication Criteria
406
Define SSID's
408
For each SSID
410
Configure/Disable Proxy Mobile IP/SSID
412
Proxy Mobile IP?
Yes
414
Configure Default Home Subnet
No
416
Configure Default VLAN ID
418
Yes
Continue?
No
420
Done

Fig. 4

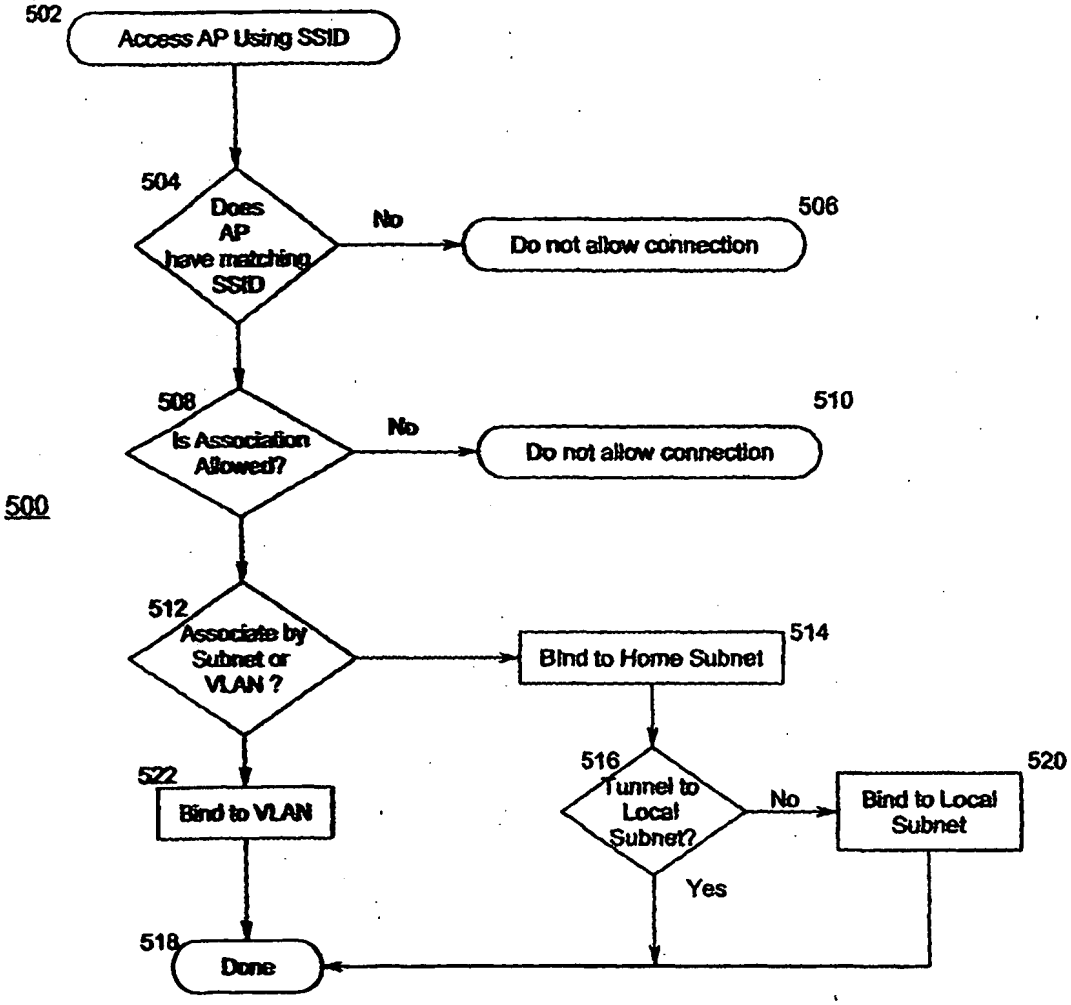

502
Access AP Using SSID
504
Does AP have matching SSID
No
506
Do not allow connection
508
Is Association Allowed?
No
510
Do not allow connection
500
512
Associate by Subnet or VLAN ?
514
Bind to Home Subnet
516
Tunnel to Local Subnet?
No
520
Bind to Local Subnet
Yes
522
Bind to VLAN
518
Done

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/22982

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04B 5/00, 7/00
US CL : 455/41.1
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/41.1, 41.2, 414.1, 418, 512, 456.4; 340/2.1, 870.02; 342/357.01, 357.06, 357.13

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
455/$.ccls., 370/$.ccls; 7 and (802.11 access point) and (proxy mobile IP)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 6,577,643 B1 (RAI et al) 10 June 2002, figs. 2-6; 32 of fig.2 or 84 of fig. 4-6; col. 5, lines 51-col. 6 line 26; col. 7 lines 34-62; col. 13 lines 42-66.	1-65
A	US 6,097,960 A (RATHINASABAPATHY et al) 01 August 2000, entire document.	1-65
A	US 6,181,927 B1 (WELLING, JR. et al) 30 January 2001, entire document.	1-65
A	US 6,181,985 B1 (GOSSMAN et al) 30 January 2001, entire document.	1-65

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 January 2004 (07.01.2004)	23 JAN 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Eugenia Logan Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)